Kaspersky Security 10 for Windows Server

Installation Guide

Program version: 10

Dear User,

Thank you for choosing our product. We hope that this documentation will help you in your work and answer your questions about this software product.

Warning! This document is the property of Kaspersky Lab AO (further referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction or distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including in translated form, is allowed only with the written permission of Kaspersky Lab.

This document and the graphics associated with it may be used exclusively for information, non-commercial or personal purposes.

This document may be amended without prior notice. For the latest version, please refer to Kaspersky Lab's website at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance or accuracy of any materials used in this document the rights to which are held by third parties, or for potential damages associated with the usage of such documents.

Revision date: 2/16/2016

http://www.kaspersky.com
http://support.kaspersky.com

Table of contents

About this Guide

The Installation Guide for Kaspersky Security 10 for Windows Server® (hereinafter referred to as Kaspersky Security, formerly Kaspersky Anti-Virus for Windows Servers Enterprise Edition) is addressed to Kaspersky Security installation and administration experts and technical support specialists whose organizations use Kaspersky Security.

You can use the information in this guide to perform the following tasks:

- Prepare Kaspersky Security for installation, install and activate the application
- Prepare Kaspersky Security for operation
- Restore or delete Kaspersky Security
- Deploy Kaspersky Security

This Guide will also help you to learn about sources of information about the application and ways to receive technical support.

In this section

In this document

The Kaspersky Security Installation Guide contains the following sections:

Sources of information about Kaspersky Security

This section lists the sources of information about the application.

Hardware and software requirements

This section lists the hardware and software requirements of Kaspersky Security

Kaspersky Security

This section describes the functions and components of Kaspersky Security.

Installation planning

This section describes Kaspersky Security administrative tools and the particulars of installing Kaspersky Security using the Setup Wizard, from the command line, via Kaspersky Security Center, and via Active Directory® group policies.

Wizard-based installation and uninstallation of the application

This section describes how to install and uninstall Kaspersky Security and Kaspersky Security Console on a protected server using the Setup Wizard. It also contains information about advanced Kaspersky Security settings and actions after installing Kaspersky Security.

Installing and uninstalling the application from the command line

This section describes the particulars of installing and uninstalling Kaspersky Security from the command line and contains examples of commands to install and uninstall Kaspersky Security from the command line, and examples of commands to add and remove Kaspersky Security components from the command line.

Installing and uninstalling the application using Kaspersky Security Center

This section contains general information about installing Kaspersky Security via Kaspersky Security Center. It also describes how to install and uninstall Kaspersky Security via Kaspersky Security Center and actions after installing Kaspersky Security.

Installation and Uninstallation through active directory group policies

This section describes installing and uninstalling Kaspersky Security via Active Directory group polices. It also contains information about actions after installing Kaspersky Security through group policies.

Migrating from a previous version of the application

This section contains information about which settings of installed programs are saved in Kaspersky Security 10 for Windows Server, their names and their values after migrating.

Checking Kaspersky Security settings Using the EICAR test virus

This section describes the EICAR test virus and how to use the EICAR test virus to verify Kaspersky Security's Real-time protection and On-demand scan features.

Kaspersky Security deployment schemes

This section contains descriptions of schemes to deploy Kaspersky Security for the protection of DAS storages, clusters, terminal servers and network storages.

Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

Glossary

This section contains a list of terms, which are mentioned in the document, as well as their respective definitions.

AO Kaspersky Lab

This section provides information about AO Kaspersky Lab.

Information about third-party code

This section provides information about third-party code used in the application.

Trademark notices

This section lists trademarks reserved to third-party owners and mentioned in the document.

Index

This section allows you to quickly find required information through the document.

Document conventions

This document uses the following conventions (see table below).

Table 1. Document conventions

Sample text	Description of document convention
Note that...	Warnings are highlighted in red and set off in a box. Warnings contain information about actions that may have undesirable consequences.
We recommend that you use...	Notes are set off in a box. Notes contain supplementary and reference information.
Example:	Examples are given in blocks against a yellow background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.
► *To configure a task schedule:*	Introductory phrases of instructions are italicized and accompanied by an arrow.

Sample text	Description of document convention
In the command line, type `help` The following message then appears: Specify the date in `dd:mm:yy` format.	The following types of text content are set off with a special font: • Text in the command line • Text of messages displayed on the screen by the application • Data that must be entered from the keyboard
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, omitting the angle brackets.

Sources of information about Kaspersky Security

This section lists the sources of information about the application.

You can select the most suitable information source, depending on the importance level and urgency of the issue.

In this section

Sources for independent retrieval of information

You can use the following sources to find information about Kaspersky Security 10 for Windows Server:

- Kaspersky Security page on the Kaspersky Lab website
- Kaspersky Security page on the Technical Support website (Knowledge Base)
- Online help
- Manuals

> If you did not find a solution to your problem, contact Kaspersky Lab Technical Support (see the section "Contacting Technical Support" on page 102).

> An Internet connection is required to use online information sources.

Kaspersky Security page on the Kaspersky Lab website

On the Kaspersky Security 10 for Windows Server page (http://www.kaspersky.com/business-security/windows-server-security), you can view general information about the application, its functions and features.

The Kaspersky Security 10 for Windows Server page contains a link to eStore. There you can purchase the application or renew your license.

Kaspersky Security page in Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Security 10 for Windows Server page in the Knowledge Base (http://support.kaspersky.com/ksws10) features articles that provide useful information, recommendations, and answers to frequently asked questions about how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only Kaspersky Security 10 for Windows Server but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Kaspersky Security documentation

Kaspersky Security 10 for Windows Server Installation Guide describes how you can perform the following tasks:

- Prepare Kaspersky Security for installation, install and activate the application
- Prepare Kaspersky Security for operation
- Restore or delete Kaspersky Security

Kaspersky Security 10 for Windows Server Administrator's Guide contains information about configuring and using Kaspersky Security.

In the Implementation Guide for Network Attached Storage Protection you can find information about configuring and using Kaspersky Security for Network Attached Storage Protection.

Discussing Kaspersky Lab applications on the forum

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users on our forum (http://forum.kaspersky.com).

On this forum you can view existing threads, leave your comments, and create new discussion threads.

Hardware and software requirements

This section lists the hardware and software requirements of Kaspersky Security.

In this section

Requirements for the server on which Kaspersky Security is deployed

Before installing Kaspersky Security, you must uninstall other anti-virus applications from the server.

You can install Kaspersky Security without uninstalling Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

Hardware requirements for the server

General requirements:

- x86-64-compatible single-core or multicore systems
- disk space requirements:
  - for installing all application components: 70 MB
  - for downloading and storing anti-virus databases of the application: 2 GB (recommended)

- for storing objects in Quarantine and in Backup: 400 MB (recommended)
- for storing logs: 1 GB (recommended)

Minimum configuration:

- Processor: 1.4 GHz single-core
- RAM: 1GB
- Drive subsystem: 4 GB of free space

Recommended configuration:

- Processor: 2.4 GHz quad-core
- RAM: 2 GB
- Drive subsystem: 4 GB of free space

Software requirements for the server

You can install Kaspersky Security on a server under a 32-bit or 64-bit Microsoft Windows operating system.

> For installation and operation of Kaspersky Security, Microsoft Windows Installer 3.1 must be installed on the server.

You can install Kaspersky Security on a server under one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later

You can install Kaspersky Security on a server under one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later

- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V® Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

You can install Kaspersky Security on the following terminal servers:

- Microsoft Remote Desktop Services based on Windows 2008 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server R2
- Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6
- Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6

Requirements for the protected network attached storage

Kaspersky Security can be used to protect the following network attached storages:

- NetApp® with one of the following operating systems:
    - Data ONTAP® 7.x and Data ONTAP 8.x in 7-mode
    - Data ONTAP 8.2.1 or higher in cluster-mode

- EMC™ Celerra™ / VNX™ with the following software:
    - EMC DART 6.0.36 or higher
    - Celerra (CAVA) Anti-Virus Agent 4.5.2.3 or higher
- EMC Isilon™ with the operating system OneFS™ 7.0 or later
- Hitachi NAS on one of the following platforms:
    - HNAS 4100
    - HNAS 4080
    - HNAS 4060
    - HNAS 4040
    - HNAS 3090
    - HNAS 3080
- IBM® NAS series IBM System Storage® N series
- Oracle® NAS Systems series Oracle ZFS Storage Appliance
- Dell™ NAS on the platform Dell Compellent™ FS8600

Requirements for the computer on which Kaspersky Security Console is installed

Hardware requirements for the computer

Recommended RAM amount: at least 128 MB.

Free disk space: 30 MB.

Software requirements for the computer

You can install Kaspersky Security Console on a computer running a 32-bit or 64-bit Microsoft Windows operating system.

The computer should have Microsoft Windows Installer 3.1 in order to support installation and operation of Kaspersky Security Console.

You can install Kaspersky Security Console on a computer running one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Microsoft Windows XP Professional with Service Pack 2 or later
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional
- Microsoft Windows 10 Enterprise / Professional

You can install Kaspersky Security Console on a computer running one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter

- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition SP2 or later
- Microsoft Windows Vista Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional
- Microsoft Windows 10 Enterprise / Professional

Kaspersky Security

Kaspersky Security 10 for Windows Server (previously Kaspersky Anti-Virus for Windows Servers Enterprise Edition) protects servers running on Microsoft® Windows® operating systems and network attached storages against viruses and other computer security threats to which servers are exposed through file exchange. Kaspersky Security is designed for use on local area networks of medium to large organizations. Kaspersky Security users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

You can install Kaspersky Security on the following servers:

- Terminal servers
- Print servers
- Application servers
- Domain controllers
- Servers that are protecting network attached storages
- File servers – these servers are more likely to get infected because they exchange files with user workstations

Kaspersky Security can be managed in the following ways:

- Via Kaspersky Security Console installed on the same server as Kaspersky Security or on a different computer
- Using commands in the command line
- Via Administration Console of Kaspersky Security Center

The Kaspersky Security Center application can also be used for centralized administration of multiple servers running Kaspersky Security.

It is possible to review Kaspersky Security performance counters for the "System Monitor" application, as well as SNMP counters and traps.

Kaspersky Security components and functions

The application includes the following components:

- Real-Time Protection.

  Kaspersky Security scans objects when they are accessed. Kaspersky Security scans the following objects:

  - Files
  - Scripts
  - Alternate file system threads (NTFS threads)
  - Master boot record and boot sectors on the local hard drives and external devices

- Server Control.

  Kaspersky Security monitors all attempts to access network file resources, enables Applications Launch Control, and blocks access to the server for remote computers if they show malicious or encryption activity.

- RPC-Network Storage Protection and ICAP-Network Storage Protection.

  Kaspersky Security installed on a server under a Microsoft Windows operating system protects network attached storages against viruses and other security threats that infiltrate the server through exchange of files.

- On-demand scan.

  Kaspersky Security runs a single scan of the specified area for viruses and other computer security threats. Kaspersky Security scans server files and RAM and also startup objects.

The following functions are implemented in the application:

- Databases and software modules update.

  Kaspersky Security downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.

- Quarantine.

  Kaspersky Security quarantines probably infected objects by moving such objects from their original location to *Quarantine*. For security purposes, objects are stored in Quarantine in encrypted form.

- Backup.

  Kaspersky Security stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.

- Administrator and user notifications

  You can configure the application to notify the administrator and users who access the protected server about events in Kaspersky Security operation and the status of Anti-Virus protection on the server.

- Importing and exporting settings.

  You can export Kaspersky Security settings to an XML configuration file and import settings into Kaspersky Security from the configuration file. All application settings or only settings for individual components can be saved to a configuration file.

- Applying templates.

  You can manually configure the security settings of a node in the server file resources tree and save the values of the configured settings to a template. This template can then be used to configure the security settings of other nodes in Kaspersky Security protection and scan tasks.

- Writing events to the event log.

  Kaspersky Security logs information about the settings of application components, the current status of tasks, events that occurred during their run, events associated with Kaspersky Security management, and information required for failure diagnostics in the Kaspersky Security operation.

- Hierarchical storage.

  Kaspersky Security can operate in hierarchical storage management mode (HSM systems). HSM systems allow data relocation between fast local drives and slow long-term data storage devices.

- Trusted zone.

  You can create a list of exclusions for protection scope or scan scope which Kaspersky Security applies to On-Demand Scan, Real-Time File Protection, Script Monitoring, and RPC-Network Storage Protection.

- Managing permissions.

  You can configure the rights of managing Kaspersky Security and the rights of managing Windows services, that are registered by the application, for users and groups of users.

In this section

Kaspersky Security application program components and their codes for the Windows Installer service

By default, \server\ks4ws_x86(x64).msi files install all Kaspersky Security application components, except for Script Monitoring component. You can include this component by activating it in the Custom installation.

The \client\ks4wstools_x86(x64).msi files install all application components from the "Administration tools" set.

The following sections list the codes of the Kaspersky Security components for the Windows Installer service. These codes can be used to define a list of components to be installed when installing Kaspersky Security from the command line.

In this section

Kaspersky Security application components

The following table contains codes for and a description of Kaspersky Security software components.

Table 2. Description of Kaspersky Security application components

Component	Code	Functions performed
Basic functionality	Core	This component contains the set of basic application functions and ensures their operation.
Applications Launch Control	APPCtrl	This component monitors user attempts to run applications and allows or denies applications launches according to the set rules. It implements the Application Launch Control task.
Anti-Virus protection	AVProtection	This component ensures anti-virus protection and contains the following components: • On-demand scan • Untrusted Hosts Blocking • Anti-Cryptor • ICAP-Network Storage Protection • RPC-Network Storage Protection • Real-Time File Protection • Script Monitoring
On-Demand Scan	Ods	This component installs Kaspersky Security system files and On-demand scan tasks (scanning of objects on the protected server upon request). If other Kaspersky Security components are specified when installing Kaspersky Security from the command line, but the Core component

Component	Code	Functions performed
		is not specified, the Core component is installed automatically.
Untrusted Hosts Blocking	HostBlocker	This component blocks access to network file resources for computers that show malicious activity. It implements the Untrusted Hosts Blocking task. This component also contains Anti-Cryptor.
Anti-Cryptor	Anticryptor	This component fills the list of untrusted computers with names of remote devices that show malicious activity. It implements the Anti-Cryptor task.
Real-Time File Protection	Oas	This component performs anti-virus scans of files on the protected server when these files are accessed. It implements the Real-Time File Protection task.
ICAP-Network Storage Protection	ICAPStorageProtection	This component implements the ICAP-Network Storage Protection task (scanning of files stored in network shared folders (network share) in network storages connected via the ICAP protocol when an attempt is made to read or modify such files from client computers).
RPC-Network Storage Protection	NetApp	This component implements the RPC-Network Storage Protection task (scanning of files stored in network shared folders (network share) in network storages connected via the RCP protocol when an attempt is made to read or modify such files from client computers).

Component	Code	Functions performed
Script Monitoring	ScriptChecker	This component scans the code of scripts created using Microsoft Windows Script Technologies. Scanning is performed when an attempt is made to run a script. This component implements the Script Monitoring task.
Use of Kaspersky Security Network	KSN	This component provides protection on the basis of Kaspersky Lab cloud technologies. It implements the KSN Usage task (sending requests to and receiving verdicts from the Kaspersky Security Network service).
Module of integration with the Kaspersky Security Center Network Agent	AKIntegration	Provides a connection between the Kaspersky Security and the Kaspersky Security Center Network Agent. You can install this component on the protected server if you intend to manage the application via the Kaspersky Security Center.
Set of "System monitor" counters.	PerfMonCounters	This component installs a set of System Monitor performance counters. Performance counters enable Kaspersky Security performance to be measured and potential bottlenecks to be localized on the server when Kaspersky Security is used with other programs.
SNMP counters and traps	SnmpSupport	This component publishes Kaspersky Security counters and traps via Simple Network Management Protocol (SNMP) in Microsoft Windows. This component may be installed on the protected server only if Microsoft SNMP is installed on the server.

Component	Code	Functions performed
Kaspersky Security icon	TrayApp	This component displays the Kaspersky Security icon in the task tray notification area of the protected server. The Kaspersky Security icon displays the status of server protection and can be used open the Kaspersky Security Console in MMC (if installed) and the **About the application** window.
Command line utility	Shell	Makes it possible to control Kaspersky Security from the command line of a protected server.

Application components of the "Administration tools" set

The following table contains codes for and a description of the "Administration tools" set of program components.

Table 3. Description of the "Administration tools" program components

Component	**Code**	**Component functions**
Kaspersky Security snap-in	MmcSnapin	This component installs the Microsoft Management Console snap-in via Kaspersky Security Console. If other components are specified during the installation of "Administration tools" from the command line, and the MmcSnapin component is not specified, the component will be installed automatically.
Help	Help	.chm help file; saved in the folder with the Kaspersky Security files. The help file can be opened from the **Start** menu.

Component	Code	Component functions
Documentation	Docs	The documents "Administrator's Guide", "Installation Guide", and "Implementation Guide for Network Attached Storage Protection" in PDF format; these are stored in the Kaspersky Security program folder; the "Administrator's Guide" can be opened from the **Start** menu.

Kaspersky Security install and uninstall log

If Kaspersky Security is installed or uninstalled using the Installation (Uninstallation) Wizard, the Windows Installer service creates an install (uninstall) log. Log file ks4ws_install_<uid>.log (where <uid> – unique 8-character log identifier) will be saved into a %temp% folder of the user from whose account the setup.exe file was launched.

If Kaspersky Security is installed or uninstalled from the command line, the install file log will not be created by default.

► *To install Kaspersky Security with the log file ks4ws.log created on disk C:\:*

- `msiexec /i ks4ws_x86.msi /l*v C:\ks4ws.log /qn EULA=1`
- `msiexec /i ks4ws_x64.msi /l*v C:\ks4ws.log /qn EULA=1`

Install and uninstall settings and their keys for the Windows Installer service

The tables provided below contain descriptions of the settings to install and uninstall Kaspersky Security, their default values, special keys for changing the values of the installation settings, and their possible values. These keys can be used in conjunction with standard keys for the command msiexec of the Windows Installer service when installing Kaspersky Security from the command line.

Table 4. Installation parameters and their keys in Windows Installer

Setting	Default value	Windows Installer key and its values	Description
Acceptance of the terms of the End User License Agreement.	Rejection of the terms of the End User License Agreement	EULA=<value> **0 –** you reject the terms of the End User License Agreement. **1 –** you accept the terms of the End User License Agreement.	You must accept the terms of the End User License Agreement to install Kaspersky Security.

Scanning of active processes and local drive boot sectors before installation (**Scan Computer for viruses**)	Do not scan	PRESCAN=<value>
		0 – scan before installation;
		1 – scan before installation
			We recommend scanning active processes and local drive boot sectors before installation because the presence of malicious code in these computer areas may interfere with the successful installation of Kaspersky Security.
			The scan may take several minutes.
			If dangerous or suspicious processes are detected during the scan, they will be deleted from the computer memory (executable files of

Setting	Default value	Windows Installer key and its values	Description
			processes are not deleted). In such cases information in applications running may be lost. Therefore we recommend that all open applications should be closed.
Destination folder	Kaspersky Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10 for Windows Server Administration tools: %Program Files%\Kaspersky Lab\Kaspersky Security 10 for Windows Server Admins Tools In the x64-bit version of Microsoft Windows: %ProgramFiles(x86)%.	INSTALLDIR=<full path to the folder>	Folder in which Kaspersky Security files will be saved during installation. A different folder can be specified.

Setting	Default value	Windows Installer key and its values	Description

Startup of Real-Time File Protection and Script Monitoring when Kaspersky Security starts (**Enable real-time protection after installation of application**)	Start	RUNRTP=<value>
		1 – start;
		0 – do not start.
			Turn on this setting to start Real-Time File Protection and Script Monitoring at Kaspersky Security startup (recommended).

Exclusions from scan as recommended by Microsoft Corporation (**Add Microsoft recommended files to exclusions list**)	Exclude	ADDMSEXCLUSION=<value>
		1 – exclude;
		0 – do not exclude.
			In the Real-Time File Protection task exclude from the protection scope objects on the server which are recommended by Microsoft Corporation for exclusion.
			Some applications on the server may become unstable when the anti-virus application intercepts or modifies files used by such applications. Microsoft Corporation

Setting	Default value	Windows Installer key and its values	Description
			includes, for example, some domain controller applications in the list of such objects.

Objects excluded from the scanning scope according to Kaspersky Lab recommendations (**Add Kaspersky Lab recommended files to exclusions list**)	Exclude	ADDKLEXCLUSION=<value>
		1 – exclude;
		0 – do not exclude.
			In the Real-Time File Protection task exclude from the protection scope objects on the server which are recommended by Kaspersky Lab for exclusion.

Exclude remote admin programs from processing (**Add objects using the not-a-virus:RemoteAdmin* mask to exclusions**)	Do not add objects using the not-a-virus:RemoteAdmin* mask to exclusions	RADMINEXCLUSION =<value> **1 –** add objects using the not-a-virus:RemoteAdmin* mask to exclusions. **0 –** do not add objects using the not-a-virus:RemoteAdmin* mask to exclusions.	When the Radmin utility is launched, Kaspersky Security detect it as being vulnerable to exploitation by fraudsters and deletes its executable module from the server drive. Kaspersky Security assigns names with the not-a-virus:RemoteAdmin* mask to such objects. If you plan to use

Setting	Default value	Windows Installer key and its values	Description
			remote administration utilities after installing Kaspersky Security, you can exclude this object from processing by the application by using the **Add objects using the not-a-virus:RemoteAdmin* mask to exclusions** installation setting. Remote administration utilities can also be excluded from processing in the Real-Time File Protection and On-Demand Scan tasks after Kaspersky Security installation (see *Kaspersky Security 10 for Windows Server. Administrator's Guide*).

Setting	Default value	Windows Installer key and its values	Description
Path to the key file (**Key**)	\server directory in the distribution kit	LICENSEKEYPATH=<key file name>	By default the installer attempts to find the license key file with .key extension in the \server folder of the distribution kit. If the \server folder contains several key files, the installer will select the key file that has the longest "service lifetime". A key file can be saved beforehand in the \server folder or by specifying another path to the key file using the **Add key** setting. You can add a key after Kaspersky Security is installed using an administration tool of your choice: for example, Kaspersky Security Console. If you do not add a key during installation of the

Setting	Default value	Windows Installer key and its values	Description
			application, Kaspersky Security will not function. Detailed information about licensing the application is provided in the *Kaspersky Security 10 for Windows ServerAdministrator 's Guide*.
Path to the configuration file	Not specified	CONFIGPATH=<configuration file name>	Kaspersky Security imports settings from the specified configuration file created in the application. Kaspersky Security does not import passwords from the configuration file, for example, account passwords for launching tasks, or passwords for connecting to a proxy server. Once the settings are imported, you will have to enter all passwords

Setting	Default value	Windows Installer key and its values	Description
			manually. If the configuration file is not specified, the application will start to work with the default settings after setup.

Enabling network connections for the Console	Disabled	ADDWFEXCLUSION=<value>
		1 – allow;
		0 – deny.
			Use this setting if Kaspersky Security is installed on a host other than the protected server. Server protection may be managed remotely using this console.
			Port 135 (TCP) is opened in the Microsoft Windows firewall, network connections for the executable file kavfsrcn.exe for remote management of Kaspersky Security are allowed, and access is granted to DCOM applications.
			When installation is

Setting	Default value	Windows Installer key and its values	Description
			complete, the users who will manage the application remotely should be added to the **KAVWSEE Administrators** group on the server; if the server runs on Microsoft Windows Server 2008, network connections for Kaspersky Security Management Service on that server should be allowed (kavfsgt.exe file). You can read more about additional configuration when the Kaspersky Security Console is installed on another computer (see page 56).

Table 5. Uninstall settings and their keys in Windows Installer

Setting	Default value	Description, Windows Installer keys and their possible values
Restoring quarantined objects	Remove	RESTOREQTN =<value> **0** – delete the quarantine content; **1** – restore the contents of the quarantine into the folder specified by RESTOREPATH parameter.

Restoring the content of backup	Remove	RESTOREBCK =<value>
		0 – delete backup content;
		1 – restore backup contents into the folder specified by RESTOREPATH parameter.

Folder for restored objects	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\	RESTOREPATH=<full path to the folder> Restored objects will be saved to the folder specified in this setting: Objects from the quarantine will be saved into the subfolder \Quarantine. Objects from Backup – into the subfolder \Backup.

Changes in the system after Kaspersky Security installation

When Kaspersky Security and Kaspersky Security Console (set of "Administration tools") are installed together, the Windows Installer service will make the following modifications on the computer:

- It will create Kaspersky Security folders on the protected server and on the computer on which the Kaspersky Security Console is installed
- Registers the Kaspersky Security service

- Creates a Kaspersky Security group of users
- Registers Kaspersky Security keys in the system register

These changes are described in the table below.

Kaspersky Security folders

Table 6. Kaspersky Security folders on the protected server

Folder	Kaspersky Security files
Folder %Kaspersky Security%; by default: In the Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\ • In the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Security for Windows Server\	Executable Kaspersky Security files (destination folder specified during installation)
Folder %Kaspersky Security%**mibs**	Management Information Base (MIB) files; these files contain a description of the counters and hooks published by Kaspersky Security via the SMNP protocol
Folder %Kaspersky Security%**x64**	64-bit versions of Kaspersky Security executable files (the folder will be created only during the installation of Kaspersky Security in the 64-bit version of Microsoft Windows)

Folder	Kaspersky Security files
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Dskm\	Kaspersky Security service files
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Update\	Files with update sources settings
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\**Update****Distribution**\	Updates of databases and application modules downloaded using Copying Updates task (the folder will be created the first time updates are downloaded using the Copying Updates task)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Reports\	Task logs and system audit log
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\**Bases****Current**\	Set of databases used at current time
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\**Bases****Backup**\	Backup copy of databases; will be overwritten each time databases are updated

Folder	Kaspersky Security files
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Bases\Temp\	Temporary files created during execution of update tasks
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Quarantine\	Quarantined objects (default folder)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Backup\	Objects in backup (default folder)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\	Objects restored from backup and quarantine (default folder for restored objects)

Table 7. Folders created during the installation of Kaspersky Security Console

Folder	Kaspersky Security files
%Folder Kaspersky Security%; by default: • In the Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\ • In the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server\	"Administration tools" files (destination folder specified during the installation of Kaspersky Security Console)

Kaspersky Security services

Kaspersky Security services start using the **Local system** (SYSTEM) account.

Table 8. Kaspersky Security services

Service	Purpose
Kaspersky Security Service (KAVFS) service	Kaspersky Security main service; manages Kaspersky Security tasks and working processes.
Kaspersky Security Management Service (KAVFSGT)	The service is intended for Kaspersky Security management through the Kaspersky Security Console.
Kaspersky Security Script Checker Service (kavfsscs)	The service processes requests for checking scripts.

Kaspersky Security groups

Table 9. Kaspersky Security groups

Group	Purpose
KAVWSEE Administrators	A group on the protected server whose users have full access to the Kaspersky Security Management Service and to all Kaspersky Security functions.

System registry keys

Table 10. System registry keys

Key	Purpose
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\KAVFS]	Kaspersky Security settings
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\Eventlog\Kaspersky Anti-Virus]	Kaspersky Security event log settings (Kaspersky Event Log)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\kavfsscs]	Script interception dispatcher service settings

Key	Purpose
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Kaspersky Security management settings
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	Performance counters settings
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\SnmpAgent] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\SnmpAgent]	SNMP Protocol Support component settings
In Microsoft Windows 32-bit version: HKEY_LOCAL_MACHINE\Software\KasperskyLab\WSEE\10.0\Trace\ In Microsoft Windows 64-bit version: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.0\Trace\	Trace log settings
In Microsoft Windows 32-bit version: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.0\CrashDump\ In Microsoft Windows 64-bit version: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.0\CrashDump\	Dump settings

Kaspersky Security processes

Kaspersky Security launches the processes described in the following table:

Table 11. Kaspersky Security processes

File name	Purpose
kavfs.exe	Kaspersky Security process
kavfswp.exe	Kaspersky Security working process
kavfsscs.exe	Kaspersky Security Script Checker process
kavtray.exe	Kaspersky Security Icon component process
Kavfsgt.exe	Kaspersky Security Management process
kavshell.exe	Command line utility process
kavfsrcn.exe	Kaspersky Security remote management process

Installation planning

This section describes Kaspersky Security administrative tools and the particulars of installing Kaspersky Security using the Setup Wizard, from the command line, via Kaspersky Security Center, and via Active Directory group policies.

Before starting to install Kaspersky Security, plan its main stages.

► *To plan the installation, take the following steps:*

1. Determine which administration tools will be used to manage and configure Kaspersky Security.
2. Identify the software components which should be installed (see page 24).
3. Select installation method.

In this section

Administration tools selection

Determine the administration tools that will be used to configure Kaspersky Security settings and to manage it. Kaspersky Security can be managed using the Kaspersky Security Console, command-line utility, and Kaspersky Security Center Administration Server.

Kaspersky Security Console

Kaspersky Security Console is an isolated snap-in added to the Microsoft Management Console. Kaspersky Security can be managed via the Kaspersky Security Console installed on the protected server or on another computer on the corporate network.

Multiple Kaspersky Security snap-ins can be added to one Microsoft Management Console opened in author mode to use it to manage the protection of multiple servers on which Kaspersky Security is installed.

Kaspersky Security Console is included in the "Administration tools" product components set.

Command line utility

You can manage Kaspersky Security from the command line of a protected server.

The command line utility is included in the Kaspersky Security program components group.

Kaspersky Security Center

If the Kaspersky Security Center application is used for centralized management of anti-virus protection of computers at your company, you can manage Kaspersky Security via the Kaspersky Security Center Administration Server.

The following components should be installed:

- **Module for integration with Kaspersky Security Center Network Agent**. This component is included in the Kaspersky Security program components group. It ensures Kaspersky Security communication with the Network Agent. Install the Module for integration with Kaspersky Security Center Network Agent onto the protected server.
- **Kaspersky Security Center Network Agent**. Install this component on each protected server. This component supports interaction between Kaspersky Security installed on the server and the Kaspersky Security Center Administration Server. The Network Agent installation file in included in the Kaspersky Security Center distribution kit folder.
- **Kaspersky Security plugin**. Additionally, install the plug-in for managing Kaspersky Security via the Administration Console on the computer where the Kaspersky Security Center Administration Server is installed. This ensures the application management interface via the Kaspersky Security Center. The plug-in installation file, \server\klcfginst.exe, is included in the Kaspersky Security distribution kit.

Selecting installation type

After specifying the application components for installation of Kaspersky Security (see section "Kaspersky Security application components and their codes for Windows Installer" on page 24), you need to select the application installation method.

Select the installation method depending on the network architecture and the following conditions:

- whether special Kaspersky Security installation settings will need to be set, or whether the recommended installation settings (see page 29) will be used
- whether the installation settings will be the same for all servers or individual to each server

Kaspersky Security can be installed interactively using the Setup Wizard or in silent mode without user participation, and invoked by running the installation package file with setup settings from the command line. A centralized remote installation of Kaspersky Security can be performed using Active Directory group policies or using the Kaspersky Security Center remote installation task.

Kaspersky Security can be installed on a single server, configured for operation and its settings saved to a configuration file; the file created can then be used to install Kaspersky Security on other servers (this possibility does not apply when the product is installed using Active Directory group policies).

Launching the Setup Wizard

The Setup Wizard can install the following:

- Kaspersky Security program components onto the protected server (see page 51) from the \server\setup.exe file of the distribution kit;
- Kaspersky Security Console from the \client\setup.exe file of the distribution kit on the protected server or another LAN host.

The installation package file can be launched from the command line with the necessary installation settings

If the installation package file is started without options, Kaspersky Security will be installed with the default settings. Kaspersky Security options can be used to modify the installation settings.

Kaspersky Security Console can be installed on the protected server and / or administrator's workstation.

Sample commands for the installation of Kaspersky Security and Kaspersky Security Console can be found in the section "Installing and Uninstalling Kaspersky Security from the command line" (see page 69).

Centralized installation via the Kaspersky Security Center

If the Kaspersky Security Center application is used in your network for managing networked computers' anti-virus protection, Kaspersky Security can be installed on multiple servers by using the Kaspersky Security Center remote installation task.

The servers on which you wish to install Kaspersky Security via Kaspersky Security Center (see page 75) may either be located in the same domain as the Administration Server as well as in a different domain, or not belong to any one domain at all.

Centralized installation using Active Directory group policies

Active Directory group policies can be used to install Kaspersky Security on the protected server. The Kaspersky Security Console can be installed on the protected server or administrator's workstation.

Kaspersky Security can be installed using just the recommended installation settings.

The servers on which Kaspersky Security is installed using Active Directory group policies must be located in the same domain and in the same organizational unit. Installation is performed at server startup before logging into Microsoft Windows.

Wizard-based installation and uninstallation of the application

This section describes how to install and uninstall Kaspersky Security and Kaspersky Security Console on a protected server using the Setup Wizard. It also contains information about advanced Kaspersky Security settings and actions after installing Kaspersky Security.

In this section

Installing using the Setup Wizard

The following sections contain information about the installation of Kaspersky Security and the Kaspersky Security Console.

► *To install and proceed with using Kaspersky Security, take the following steps:*

1. Install Kaspersky Security on the protected server (see section "Installing Kaspersky Security on a protected server" on page 51).

2. Install Kaspersky Security Console on the computers from which you intend to manage Kaspersky Security (see section "Installing Kaspersky Security Console" on page 55).

3. If the Kaspersky Security Console has been installed on a computer other than the protected server, configure additional settings to allow Console users to manage Kaspersky Security via the Console (see section "Advanced settings after installation of Kaspersky Security Console on another computer" on page 56).

4. Perform actions after installing Kaspersky Security (on page 61).

In this section

Installing Kaspersky Security on a protected server

Before installing Kaspersky Security, take the following steps:

- Make sure no other anti-virus programs are installed on the server. You can install Kaspersky Security without uninstalling Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
- Make sure that the account which you are using to start the Setup Wizard is registered in the administrators group on the protected server.

After completing the actions described above, proceed with the installation procedure. Following the Setup Wizard instructions, specify the settings for Kaspersky Security installation. The Kaspersky Security installation process can be stopped at any step of the Setup Wizard. To do so, press the **Cancel** button in the Setup Wizard window.

You can read more about the installation (uninstallation) settings (see page 29).

► *To install Kaspersky Security using an installation wizard:*

1. Start the welcome shell file on the server.
2. In the window that opens, in the **Installation** section, click the **Install Kaspersky Security** link.

3. In the welcome screen of the Kaspersky Security Setup Wizard, click the **Next** button.

   The **End User License Agreement** window opens.

4. Review the terms of the License Agreement and select **I accept the terms of End User License Agreement** in order to proceed with the installation. Press the **Next** button.

   If the server has Kaspersky Anti-Virus for Windows Servers Enterprise Edition installed, the **Previous version of the program detected** window will open.

   If previous versions of the program are not detected, proceed to step 6 of these instructions.

5. To upgrade from the previous version of the application, click the **Install** button. The Setup Wizard will upgrade application to Kaspersky Security and save compatible settings in the new version (see section "Migration to Kaspersky Security from an earlier version of the application" on page 87). On the upgrade completion, wizard will open the **Installation completion** window (proceed to the Step **15** of these instructions).

   The **Quick scan of the computer before installation** window opens.

6. In the **Quick scan of the computer before installation**, check the box **Scan computer for viruses** to scan system memory and boot sectors of the local server drives for threats. Press the **Next** button. On completion of the scanning procedure the wizard will open a window reporting Quick scan results.

   This window displays information about scanned server objects: the total number of scanned objects, the number of threat types detected, the number of infected or probably infected objects detected, the number of dangerous or suspicious processes removed from memory by Kaspersky Security, and the number of dangerous or suspicious processes that the application was unable to remove.

   To see exactly which objects were scanned, press the **List of processed objects** button.

7. Press the **Next** button in the **Quick scan of the computer before installation** window.

   The **Installation type** window opens.

8. Select one of the following options:

   - **Recommended configuration**, to install all the components of Kaspersky Security, except for the Script scanning component. Go to step 11 of this instruction.

   - **Custom installation**, to select the components for installation from the list of Kaspersky Security features.

9. If **Custom installation** is selected, the **Custom installation** window opens.

   All components of Kaspersky Security, except for Script Monitoring, are included in the installation list by default.

   > The SNMP protocol support component of Kaspersky Security will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the server.

   Select the components to be installed. To cancel all changes, press the **Reset** button in the **Custom installation** window. Press the **Next** button.

10. In the opened **Select destination folder** window:

    - If required, specify a folder to which Kaspersky Security files will be copied.

    - If required, review the information about available space on the local drives, by clicking **Disk** button.

    Press the **Next** button.

11. In the **Advanced installation settings** window, configure the following installation settings:

    - **Enable Real-time protection after installing the application.**

    - **Add file exclusions recommended by Microsoft**.

    - **Add Kaspersky Lab recommended files to exclusions list**.

    - **Add objects using a not-a-virusRemoteAdmin* mask to exclusions list**.

    Press the **Next** button.

12. In the opened **Import settings from configuration file** window:

    To import Kaspersky Security settings from an existing configuration file created in Kaspersky Security 8.0 for Windows Servers Enterprise Edition, specify the configuration file. Press the **Next** button.

13. In the **Activation of the application** window, do one of the following:

    - If you want to activate the application, specify a Kaspersky Security key file for application activation.
    - If you want to activate the application later, press the **Next** button.
    - If a key file has been saved beforehand in the \server folder of the distribution kit, the name of this file will be displayed in the **Key** field.
    - To add the key using a key file stored in another folder, specify the key file.

      > You cannot activate the application using an activation code via Setup Wizard. If you want to activate the application using activation code, you need to enter the code after installation. Detailed information about the activation of application is provided in the *Kaspersky Security 10 for Windows Server Administrator's Guide*.

      Once the key file is added, license information will be shown in the window. Kaspersky Security displays the calculated date of license expiry. The license term runs from the time when you add a key and expires no later than the key file expiry date.

    Click **Next** button to apply the key in the application.

14. In the **Ready to install** window, press the **Install** button. The wizard will start the installation of Kaspersky Security components.

15. The **Installation complete** window opens when installation is completed.

16. Check the **View Release Notes** box to view information about the release after the Setup Wizard is done.

17. Click **OK**.

Setup Wizard windows will be closed. Once installation is completed, Kaspersky Security is ready for use if you have added the activation key.

Installing Kaspersky Security Console

Follow the instructions of the Setup Wizard to adjust the installation settings for Kaspersky Security Console. The installation process can be stopped at any step of the wizard. To do so, press the **Cancel** button in the wizard window.

► *To install Kaspersky Security Console:*

1. Make sure that the account from which you are running the Setup Wizard is included in the administrators group on the computer.

2. Run the greeting program file named setup.exe on the computer.

   The welcome window opens.

3. Click on the **Install Kaspersky Security Console** link.

   The Setup Wizard greeting window opens. Press the **Next** button.

4. Review the terms of the **End User License Agreement** in the opened window, and select **I accept the terms of End User License Agreement** in order to proceed with the installation. Press the **Next** button.

5. In the **Installation type** window that opens, select one of the following options:

   - **Full installation** to install the complete set of "Administration tools" components, which includes the Kaspersky Security Console, help file, and application documentation. Go to step 7 of this instruction.

   - **Custom installation** manually selects the components from the list. Press the **Next** button.

   > You can read more about the components of Kaspersky Security (see page 24).

6. If **Custom installation** is selected, the **Custom installation** window opens.

   All the components of the "Administration tools" set are included in the list of components to be installed by default. Select the components to be installed. Press the **Next** button.

7. In the opened **Select destination folder** window:

   If required, specify a different folder in which the files being installed should be saved. Press the **Next** button.

8. In the **Advanced installation settings** window that opens:

   If you intend to use the Kaspersky Security Console to manage Kaspersky Security installed on a remote computer, select the **Allow remote access** check box. Press the **Next** button.

9. In the **Ready to install** window, press the **Install** button. The wizard will begin installing the selected components.

10. The **Installation complete** window opens when the installation is completed.

11. Click **OK**.

The Setup Wizard window will close. Kaspersky Security Console will be installed on the protected server.

If the "Administration tools" set has been installed on a different computer rather than on the protected server, adjust the advanced settings (see section "Advanced settings after installation of Kaspersky Security Console on another computer" on page 56).

Advanced settings after installation of Kaspersky Security Console on another computer

If the Kaspersky Security Console has been installed on a different computer other than the protected server, perform the actions described below to allow users to manage Kaspersky Security remotely:

- Add Kaspersky Security users to the KAVWSEE Administrators group on the protected server.
- If the protected server is running on Microsoft Windows Server 2008 / 2012 / 2012 R2, allow network connections for the Kaspersky Security Management Service (kavfsgt.exe) on this server.
- If during installation of Kaspersky Security Console on a computer running Microsoft Windows the setting **Allow network connections for Kaspersky Security Console** was not enabled, manually allow network connections for Kaspersky Security Console through the computer's firewall.

In this section

About access permissions for Kaspersky Security Management Service

The list of Kaspersky Security services can be reviewed (see section "Changes in the system after Kaspersky Security installation" on page 39).

During installation, Kaspersky Security registers Kaspersky Security Management Service (KAVFSGT). To manage the application via Kaspersky Security Console installed on a different computer, the account whose permissions are used to connect to Kaspersky Security must have full access to Kaspersky Security Management Service on the protected server.

By default, access to the Kaspersky Security Management Service is granted to users of the Administrators group on the protected server and users of the KAVWSEE Administrators group created on the protected server during Kaspersky Security installation.

You can manage Kaspersky Security Management Service only via the **Services** snap-in of Microsoft Windows.

You cannot allow or block user access to Kaspersky Security Management Service by configuring Kaspersky Security.

You can connect to Kaspersky Security from a local account if an account with the same name and password is registered on the protected server.

Enabling network connections for Kaspersky Security Management Service

> The names of settings may vary under different Windows operating systems.

To establish a connection between Kaspersky Security Console and the Kaspersky Security Management Service, you need to allow network connections for the service through the firewall on the protected server.

> Network connections have to be configured if Kaspersky Security runs under Microsoft Windows Server 2003 / 2008 / 2012 / 2012 R2.

► *To allow network connections for Kaspersky Security Management Service on the protected server:*

1. On the protected server running Windows Server select **Start** → **Control Panel** → **Security** → **Windows Firewall**.
2. In the **Windows firewall settings** window, select the **Change settings** command.
3. In the list of predefined exceptions on the **Exceptions** tab check the flags: **COM + Network access**, **Windows Management Instrumentation (WMI)** and **Remote Administration**.
4. Click the **Add Program** button.
5. Specify kavfsgt.exe file in the **Add Program** dialog window. This is located in the folder specified as the destination folder during installation of Kaspersky Security.
6. Click **OK**.
7. Press the **OK** button in the **Windows Firewall settings** dialog window.

Network connections for Kaspersky Security Management Service are now enabled.

Permission for network connections for Kaspersky Security Console running Microsoft Windows

The names of settings may vary under different Windows operating systems.

The Kaspersky Security Console uses the DCOM protocol to receive information about application events (objects scanned, tasks completed, etc.) from the Kaspersky Security Management Service on a remote server.

If the computer on which Kaspersky Security Console is installed runs on Microsoft Windows XP SP2 or higher / Vista / 7 / 8 / 8.1, network connections have to be allowed via the firewall on this computer, in order to establish a connection between Kaspersky Security Console and Kaspersky Security Management Service.

► *To establish connections between the Console and Kaspersky Security Management Service:*

1. Make sure that anonymous remote access to COM applications is allowed (but not remote launch and activation of COM applications).
2. In the Windows firewall open port 135 (TCP) and allow network connections for the executable file of the Kaspersky Security remote management process kavfsrcn.exe. The computer on which Kaspersky Security Console is installed exchanges information via port TCP 135 with the protected server on which Kaspersky Security is installed.

If Kaspersky Security Console was opened while you were configuring the connection between the protected server and the computer on which Kaspersky Security Console is installed, close Kaspersky Security Console, wait for the Kaspersky Security remote management process kavfsrcn.exe to end, and restart the Console. The new connection settings will be applied.

► *To allow anonymous remote access to COM applications, take the following steps:*

1. On the computer on which Kaspersky Security Console is installed, open the **Component Services** console: select **Start** → **Run**, type **dcomcnfg**, and click **OK**.
2. Expand the **Computers** node in the **Component Services** console of the computer, open the context menu of the **My Computer** node and select the **Properties** command.

3. On the **COM Security** tab of the **Properties** window, click the **Edit limits** button in the **User rights** group of settings.

4. Make sure that the **Allow Remote Access** check box is selected for the **ANONYMOUS LOGON** user in the **Allow remote access** window.

5. Click **OK**.

► *To open TCP port 135 in the Windows firewall and to allow network connections for the Kaspersky Security remote management process executable file:*

1. Close Kaspersky Security Console on the remote computer.

2. Perform the following actions depending on the computer's operating system:

   - In Microsoft Windows XP SP2 or higher:

     a. Select **Start** → **Control Panel** → **Windows Firewall**.

     b. In **Windows Firewall** window press the **Add Program** on the **Exclusions** tab.

   - In Microsoft Windows Vista:

     a. Select **Start** > **Control panel** > **Windows firewall** and in the **Windows firewall** window select the command **Change settings**.

     b. In **Windows Firewall** window (or **Windows Firewall settings**) click the **Add port** button on the **Exclusions** tab.

     c. In the **Name** field specify the part name RPC (TCP/135) or enter another name, for example Kaspersky Security DCOM, and specify port number (135) in the **Port name** field.

     d. Select **TCP** protocol.

     e. Click **OK**.

     f. Press the **Add Program** button on the **Exclusions** tab.

   - In Microsoft Windows 7 :

     a. Select **Start** → **Control panel** → **Windows firewall**, in the **Windows firewall** window select **Allow run of a program or component through Windows firewall**.

     b. In the **Allow programs to communicate through Windows Firewall** window click the **Allow another program...** button.

3. Specify kavfsgt.exe file in the **Add Program** window. This is located in the folder specified as a destination folder during the installation of Kaspersky Security Console using MMC. By default the full path to the file is as follows:

   - In the Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\kavfsrcn.exe
   - In the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for Windows Server Admins Tools\kavfsrcn.exe.

4. Click **OK**.

5. Click the **OK** button in the **Windows firewall** (**Windows firewall settings**) window.

Actions after installing Kaspersky Security

Kaspersky Security starts the protection and scan tasks immediately after installation if you have activated the application. If **Enable real-time protection after installation of application** was selected during installation of Kaspersky Security, Kaspersky Security scans server file system objects when they are accessed. If the Script monitoring component was installed during custom installation, Kaspersky Security scans the program code of all scripts when they are run. Kaspersky Security will run the Critical Areas Scan task every Friday at 20:00.

We recommend taking the following steps after installing Kaspersky Security:

- Starting the Kaspersky Security databases update task. After installation Kaspersky Security will scan objects using the database included in the application distribution kit.

  > We recommend updating Kaspersky Security databases immediately since they may be out of date.

  The application will then update the databases every hour according to the default schedule configured in the task.

- Run a Critical Areas Scan of the server if no anti-virus software with real-time file protection was installed on the protected server before installing Kaspersky Security.

- Configure administrator notifications about Kaspersky Security events.

Detailed information about starting and configuring the settings of update and scan tasks, as well as instructions on configuring an administrator notification are provided in the *Kaspersky Security 10 for Windows Server Administrator's Guide*.

In this section

Starting Kaspersky Security databases update task

To update databases after installation of the application, you need to:

1. In the settings of the Database Update task, configure a connection with the source of updates – **Kaspersky Lab HTTP or FTP update servers**.
2. Start the Database Update task.

► *To configure the connection with the Kaspersky Lab's update servers, in the Database Update task:*

1. Open Kaspersky Security Console on the PC. To do this, select **Start** → **Programs** → **Kaspersky Security 10 for Windows Server** → **Administration tools** → **Kaspersky Security Console**.
2. If Kaspersky Security Console has been started on a computer other than the protected server, connect to the protected server: open the context menu on the **Kaspersky Security** node in the Console tree, select **Connect to another computer**, then in the **Select computer** dialog box select **Another computer**, and enter the network name of the protected server in the input field.

   > If the user account that you used to sign into Microsoft Windows does not have sufficient privileges to access the Kaspersky Security Management Service on the server, specify a user account that has such permissions. You can read about which accounts can be given access to Kaspersky Security Management Service (see section "About access permissions for Kaspersky Security Management Service" on page 57).

   The Kaspersky Security Console window opens.

3. In the Kaspersky Security Console tree, expand the **Update** node.

4. Select the **Database Update** subnode.

5. Click the **Properties** link in the details pane.

6. In the **Task settings** window that opens, open the **Connection settings** tab.

7. Do the following:

    a. If Web Proxy Auto-Discovery Protocol (WPAD) is not configured on your network to detect proxy server settings automatically in the LAN, specify the proxy server settings: in the **Proxy server settings** section, select **Use specified proxy server settings**, enter the address in the **Address** field, and enter the port number for the proxy server in the **Port** field.

    b. If your network requires authentication when accessing the proxy server, select the necessary authentication method in the drop-down list of the **Proxy server authentication settings** section:

    - **Use NTLM authentication** if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Security will use the user account specified in the task to access the proxy server (by default the task will run under the **Local system** (**SYSTEM**) user account).
    - **Use NTLM authentication with name and password** if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Security will use the account specified for accessing the proxy server.

      Enter username and password or select a user from the list.
    - **Use user name and password** to select basic authentication. Enter username and password or select a user from the list.

8. Click **OK** in the **Task settings** window.

The settings for connecting with the update source in the Database Update task will be saved.

► *To run the Database Update task:*

1. In the Kaspersky Security Console tree, expand the **Update** node.
2. In the context menu on the **Database Update** subnode, select the **Start** command.

   The Database Update task will start.

After the task has successfully completed, you can view the release date of the latest database updates installed in the **Kaspersky Security** node.

Critical Areas Scan

After you have updated the Kaspersky Security databases, scan the server for malware using the Critical Areas Scan task.

► *To run the Critical Areas Scan task:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. In the context menu of the **Critical Areas Scan** subnode, select the **Start** command.

   The task starts; the task status *Running* is displayed in the workspace.

► *To view the task log,*

in the details pane of the **Critical areas scan** node, click the **Open log** link.

Modifying the set of components and repairing Kaspersky Security

Kaspersky Security components can be added or removed. You need to stop the Real-Time File Protection task before you can remove the Real-Time File Protection component. There is no need otherwise to stop the Real-Time Protection or Kaspersky Security service.

► *To modify the set of Kaspersky Security components:*

1. Start the welcome shell file (setup.exe) on the protected server that has Kaspersky Security installed.
2. In the window that opens, in the **Installation** section, click the **Install Kaspersky Security** link.

   The Setup Wizard's **Modify, repair or remove installation** window opens.
3. Select **Modify components set**. Press the **Next** button.

   The **Custom installation** window opens.
4. In the **Custom installation** window, in the list of available components, select the components that you want to add to Kaspersky Security or that you want to remove. To do this, perform the following actions:

   - To install new components, click the ✖▾ button next to the name of the selected component, and in the context menu select:
     - **Component will be installed on local hard drive** if you want to install one component
     - **Component and its subcomponents will be installed on local hard drive** if you want to install a group of components
   - To remove previously installed components, click the 🖴▾ button next to the name of the selected component, and in the context menu select **Component will be unavailable**.

   Press the **Install** button.
5. In the **Ready to install** window, confirm the change to the set of application components by clicking the **Install** button.
6. In the window that opens upon completion of installation, click the **OK** button.

The set of Kaspersky Security components will be modified based on the specified settings.

If problems occur in the operation of Kaspersky Security (Kaspersky Security crashes; tasks crash or do not start), it is possible to attempt to restore the Kaspersky Security. You can perform a restore while saving the current settings of Kaspersky Security, or you can select an option to reset all Kaspersky Security settings to their default values.

► *To restore Kaspersky Security after an abnormal termination:*

1. Start the welcome shell file (setup.exe) on the protected server that has Kaspersky Security installed.
2. In the window that opens, in the **Installation** section, click the **Install Kaspersky Security** link.

   The Setup Wizard's **Modify, repair or remove installation** window opens.
3. Select **Repair installed components**. Press the **Next** button.

   This opens the **Repair installed components** window.
4. In the **Repair installed components** window, select the **Restore recommended application settings** check box if you want to reset the configured application settings and restore Kaspersky Security with its default settings. Press the **Install** button.
5. In the **Ready to repair** window, confirm the application repair by clicking the **Install** button.
6. In the window that opens upon completion of the restore, click the **OK** button.

Kaspersky Security will be restored based on the specified settings.

Uninstallation using the Setup Wizard

This section contains instructions on removing Kaspersky Security and the Kaspersky Security Console from a protected server using the Setup Wizard.

In this section

Uninstalling Kaspersky Security from a protected server

> The names of settings may vary under different Windows operating systems.

Kaspersky Security can be uninstalled from the protected server using the Setup / Uninstallation Wizard.

The server may need to be rebooted after uninstalling Kaspersky Security from the protected server. Rebooting can be postponed.

► *To uninstall Kaspersky Security:*

1. In the **Start** menu, select **All programs** → **Kaspersky Security 10** → **Modify or Remove**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.

2. Select **Remove application components**. Press the **Next** button.

   The **Advanced application uninstallation settings** window opens.

3. If necessary, in the **Advanced application uninstallation settings** window:

   - Select the **Export Quarantine objects** check box in order for Kaspersky Security to export objects that have been quarantined. The check box is cleared by default.

   - Check the **Export Backup objects** checkbox, in order to export objects from Kaspersky Security Quarantine. The check box is cleared by default.

   - Click the **Save to** button and select the folder to which you want to export restored objects. By default, the objects will be exported to %ProgramData%\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Uninstall.

   Press the **Next** button.

4. In the **Ready to uninstall** window, confirm removal by clicking the **Uninstall** button.

5. In the window that opens upon completion of removal, click the **OK** button.

Kaspersky Security will be removed from the protected server.

Uninstalling Kaspersky Security Console

The names of settings may vary under different Windows operating systems.

You can uninstall Kaspersky Security Console from the computer using the Setup / Uninstallation Wizard.

After you have uninstalled Kaspersky Security Console, you do not need to restart the computer.

► *To uninstall Kaspersky Security Console:*

1. In the **Start** menu, select **All programs** → **Kaspersky Security 10** → **Administration tools** → **Modify or Remove**.
2. The wizard's **Modify, repair or remove installation** window opens.

   Select **Remove application components** and press the **Next** button.
3. The **Ready to uninstall** window opens. Press the **Remove** button.

   The **Uninstallation complete** window opens.
4. Click **OK**.

Removal is now complete, and the Setup Wizard closes.

Installing and uninstalling the application from the command line

This section describes the particulars of installing and uninstalling Kaspersky Security from the command line and contains examples of commands to install and uninstall Kaspersky Security from the command line, and examples of commands to add and remove Kaspersky Security components from the command line.

In this section

About installing and uninstalling Kaspersky Security from the command line

Kaspersky Security can be installed or uninstalled, and its components added or removed, by running the \server\ks4ws_x86(x64).msi installation package files from the command line after the installation settings have been specified using keys.

The "Administration tools" set can be installed on the protected server or on another computer on the network to work with Kaspersky Security Console locally or remotely. To do this, use the \client\ks4wstools.msi installation package.

Perform the installation using the rights of an account that is included in the administrators group on the computer on which the application is installed.

If one of the \server\ks4ws_x86(x64).msi files is run on the protected server without additional keys, Kaspersky Security will be installed with the recommended installation settings (see page 29).

The set of components to be installed can be assigned using the ADDLOCAL key by listing the codes for the selected components or sets of components as its values.

Example commands for installing Kaspersky Security

This section provides examples of commands used to install Kaspersky Security.

On computers running a 32-bit version of Microsoft Windows, run the files with the x86 suffix in the distribution kit. On computers running a 64-bit version of Microsoft Windows, run the files with the x64 suffix in the distribution kit.

Detailed information about use of the standard commands and keys of the Windows Installer service is provided in the documentation supplied by Microsoft.

Examples for Kaspersky Security installation from file setup.exe

► *To install Kaspersky Security with the recommended installation settings in the mode without interaction with the user, run the following command:*

```
\server\setup.exe /s /p EULA=1
```

► *To install Kaspersky Security with the following settings:*

- install Real-Time File Protection and On-Demand Scan components only;
- do not run Real-Time Protection when starting Kaspersky Security;
- do not exclude from the scan files recommended for exclusion by Microsoft Corporation;

perform the following command:

```
\server\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

▶ *Examples of commands used for installation: running the .msi file of an installation package*

▶ *To install Kaspersky Security with the recommended installation settings in the mode without interaction with the user, run the following command:*

```
msiexec /i ks4ws.msi /qn EULA=1
```

▶ *To install Kaspersky Security with the recommended installation settings; display the installation interface, run the following command:*

```
msiexec /i ks4ws.msi /qf EULA=1
```

▶ *In order to install Kaspersky Security with activation using the key file C:\0000000A.key:*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
```

▶ *To install Kaspersky Security with a preliminary scan of active processes and boot sectors of the local disks, run the following command:*

```
msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1
```

▶ *To install Kaspersky Security while saving its files in the destination folder C:\KSWS, execute the following command:*

```
msiexec /i ks4ws.msi INSTALLDIR=C:\KSWS /qn EULA=1
```

▶ *To install Kaspersky Security: save the installation log file with name ksws.log in the folder in which the msi file of the Anti-Virus installation package is stored, and execute the following command:*

```
msiexec /i ks4ws.msi /l*v ksws.log /qn EULA=1
```

▶ *To install Kaspersky Security Console, run the following command:*

```
msiexec /i ks4wstools.msi /qn EULA=1
```

▶ *To install Kaspersky Security with activation using the key file C:\0000000A.key: add objects matching the not-a-virus:RemoteAdmin* mask to exclusions; configure Kaspersky Security according to the settings described in the configuration file C:\settings.xml, and execute the following command:*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key
RADMINEXCLUSION=1 CONFIGPATH=C:\settings.xml /qn EULA=1
```

See also

Actions after installing Kaspersky Security 72

Install and uninstall settings and their keys for the Windows Installer service 29

Actions after installing Kaspersky Security

Kaspersky Security starts the protection and scan tasks immediately after installation if you have activated the application. If you selected **Enable real-time protection after installation of application** during installation of Kaspersky Security, Kaspersky Security scans server file system objects when they are accessed. If the Script monitoring component was installed during custom installation, Kaspersky Security scans the program code of all scripts when they are run. Kaspersky Security will run the Critical Areas Scan task every Friday at 20:00.

We recommend taking the following steps after installing Kaspersky Security:

- Starting the Kaspersky Security databases update task. After installation Kaspersky Security will scan objects using the database included in its distribution kit. We recommend updating Kaspersky Security database immediately. To do so, you must run the Database Update task. The database will then be updated every hour according to the default schedule.

  For example, you can run the Database Update task by running the following command:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
  /PROXYUSER:inetuser /PROXYPWD:123456
  ```

  In this case, updates of Kaspersky Security databases are downloaded from Kaspersky Lab update servers. Connection to an update source is established via a proxy server (proxy server address: proxy.company.com, port: 8080) using built-in Windows NTLM authentication to access the server under an account (username: inetuser; password: 123456).

  For more details on managing Kaspersky Security from the command line, see the *Administrator's Guide for Kaspersky Security 10 for Windows Server.*

- Run a Critical Areas scan of the server if no anti-virus software with real-time file protection was installed on the protected server before installing Kaspersky Security.

► *To start the Critical Areas Scan task using command line:*

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

This command saves the task log in the file scancritical.log contained in the current folder.

- Configure administrator notifications about Kaspersky Security events (see the *Administrator's Guide for Kaspersky Security 10 for Windows Server*).

Adding / uninstalling components. Sample commands

If you want to add new components to the list of previously installed Kaspersky Security components, make sure that the list of values for the ADDLOCAL key contains not only the codes for the components that you want to install but also the codes for the components that are already installed. Otherwise, installed components will be removed.

The On-Demand Scan component is installed automatically. You do not need to specify it in the list of ADDLOCAL key values by adding or deleting Kaspersky Security components.

► *To add the Script Monitoring component to already installed components, run the following command:*

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,ScriptChecker /qn EULA=1
```

or

```
\server\setup.exe /s /p "ADDLOCAL=Oas,ScriptChecker EULA=1"
```

Uninstalling Kaspersky Security. Sample commands

► *To uninstall Kaspersky Security from the protected server, run the following command:*

```
msiexec /x ks4ws.msi /qn EULA=1
```

► *To uninstall Kaspersky Security Console, run the following command:*

```
msiexec /x ks4wstools.msi /qn EULA=1
```

Return codes

The below table contains a list of return codes from the command line.

Table 12. Return codes

Code	Description
25001	Insufficient rights to install the application.
25002	A previous version of the application has not been removed.
25003	Application being installed does not match the operating system's word size (32-bit vs. 64-bit).
25004	Incompatible application detected.

Installing and uninstalling the application using Kaspersky Security Center

This section contains general information about installing Kaspersky Security via Kaspersky Security Center. It also describes how to install and uninstall Kaspersky Security via Kaspersky Security Center and actions after installing Kaspersky Security.

In this section

General information on installing via Kaspersky Security Center

You can install Kaspersky Security via Kaspersky Security Center using the remote installation task.

After the remote installation task is complete, Kaspersky Security will be installed with identical settings on several computers.

All servers can be combined in a single administration group and a group task created to perform Kaspersky Security installation on the servers of this group.

You can create a task to remotely install Kaspersky Security on a set of computers that are not in the same administration group. When creating this task you must generate a list of the individual computers on which Kaspersky Security should be installed.

Detailed information on the remote installation task is provided in the *Kaspersky Security Center Administrator's Guide*.

Rights to install or uninstall Kaspersky Security

The account specified in the remote installation (removal) task must be included in the administrators group on each of the protected servers in all cases except those described below:

- If the Kaspersky Security Center Network Agent is already installed on computers on which Kaspersky Security is to be installed (no matter in which domain the computers are located and whether they belong to any domain).

  > If the Network Agent is not yet installed on the servers, you can install it with Kaspersky Security using a remote installation task. Before installing the Network Agent, make sure that the account that you want to specify in the task is included in the administrators group on each of the servers.

- All computers on which you want to install Kaspersky Security are in the same domain as the Administration Server, and the **Administration Server** is registered under the **Domain Admin** account (if this account has local administrator's rights on the computers within the domain).

By default, when using the **Forced installation** method, the remote installation task is run from the account from which the Administration Server runs.

When working with group tasks or with tasks for sets of computers in the forced installation (uninstallation) mode, an account should have the following rights on a client computer:

- right to remote run of applications;
- with rights to the **Admin$** resource;
- with the right **Entry as a service**.

Kaspersky Security installation procedure via Kaspersky Security Center

Detailed information about generating an installation package and creating a remote installation task is provided in the *Kaspersky Security Center Implementation Guide*.

If you intend to manage Kaspersky Security via Kaspersky Security Center in the future, make sure that the following conditions are met:

- The computer where the Kaspersky Security Center Administration Server is installed also has the Kaspersky Security Administration Plug-in installed (\server\klcfginst.exe file in the Kaspersky Security distribution kit).
- Kaspersky Security Center Network Agent is installed on protected servers. If Kaspersky Security Center Network Agent is not installed on the protected servers, you can install it together with Kaspersky Security using a remote installation task.

Servers can also be combined into an administration group beforehand in order to later manage the protection settings using Kaspersky Security Center policies and group tasks.

► *To install Kaspersky Security with the help of remote installation, carry out the following:*

1. Launch Administration Console of Kaspersky Security Center.
2. In Kaspersky Security Center, expand the **Remote installation** node and in the **Installation Packages** subnode create a new installation package, specifying the ks4ws.kud file from the distribution kit as the installation package file.
3. If required, in the properties of the created installation package, change the set of Kaspersky Security components to be installed (see section "Modifying the set of components and repairing Kaspersky Security" on page 64). If required, change the default installation settings (see section "Install and uninstall settings and their keys for the Windows Installer service" on page 29).

   In Kaspersky Security Center, expand the **Remote installation** node and in the **Installation packages** subnode in the workspace open the context menu of the created Kaspersky

Security installation package and select **Properties**. In the **Properties:<name of installation package>** window in the **Settings** section, do the following:

a. In the **Components to install** group of settings check boxes next to the names of the Kaspersky Security components you wish to install.

b. In order to indicate a destination folder other than the default one, specify the name of the folder and the path to it in the **Destination folder** field.

The path to the destination folder may contain system environment variables. If such folder does not exist on the server, it will be created.

c. In the **Advanced installation settings** group, create the following settings:

- Scan the computer for viruses before starting the installation.
- Enable continuous protection after installing the application.
- Add file exclusions recommended by Microsoft.
- Consider the exclusions recommended by Kaspersky Lab.
- Add objects using the not-a-virus:RemoteAdmin* mask to exclusions.

d. To import Kaspersky Security settings from an existing configuration file created in Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition, specify the configuration file.

e. In the **Properties: <name of installation package>** dialog window, click **OK**.

4. In the **Installation Packages** node create a task to remotely install Kaspersky Security on the selected computers (administration group). Configure task settings.

   To learn more about creating and configuring remote installation tasks, see *Administrator's Guide for Kaspersky Security Center*.

5. Run the remote installation task for Kaspersky Security.

Kaspersky Security will be installed onto the computers specified in the task.

See also

Actions after installing Kaspersky Security 79

Checking Kaspersky Security functions Using the EICAR test virus 90

Actions after installing Kaspersky Security

After Kaspersky Security is installed we recommend that Kaspersky Security databases on the servers are updated, and that a critical areas scan of the server is performed, if no anti-virus applications with enabled Real-Time Protection function were installed on the servers before the installation of Kaspersky Security.

If the servers on which Kaspersky Security was installed are unified in a single administration group in the Kaspersky Security Center, you can perform these tasks using the following methods:

1. Create Database Update tasks for the group of servers on which Kaspersky Security was installed. Set Kaspersky Security Center Administration Server as the update source.

2. Create a group On-Demand Scan task with the *Critical Areas Scan task* status. Kaspersky Security Center evaluates the security status of each server in the group based on the results of the execution of this task, not the Critical Areas scan task.

3. Create a new policy for the group of servers. In the properties of the created policy, on the **System tasks** tab, deactivate the scheduled start of system scan tasks as required and the database update tasks on the administration group servers.

You can also configure administrator notifications about Kaspersky Security events (see the *Administrator's Guide for Kaspersky Security 10 for Windows Server*).

Detailed information about configuring Kaspersky Security settings via Kaspersky Security Center is provided in the *Kaspersky Security 10 for Windows Server Administrator's Guide*.

In this section

Creating and launching an "Database Update" group task

After specifying the updates source with the policy, create and start a group task to update the Kaspersky Security databases. During the creation of this task it is possible to configure its scheduled launch as **After Administration Server has retrieved updates**.

► *To create an application database update group task, proceed as follows:*

1. Launch the group task creation wizard: in the Kaspersky Security Center Administration Console tree select the **Managed computers** node, select the group whose servers should create a task, open the context menu on the nested folder **Tasks** and select **New** → **Task**.
2. Enter the name of the task in the **Specify task name** window of the task creation wizard, for example Updating databases on the group servers.
3. In the **Task type** window under the heading **Kaspersky Security 10**, select the type of the task to be created: Database Update.
4. In the **Settings** window, select **New**.
5. In the **Update source** window, select the **Kaspersky Security CenterAdministration Server** item.
6. In the **Schedule** window, check the **Run by schedule** box and in the **Frequency** list select the item **After Administration Server has retrieved updates**.
7. In the **Finish** window of the task creation wizard press the **Ready** button.

A group task for application database updates will be created.

Creating and launching a group server scan task and assigning the "Critical Areas Scan task" status to it

► *To create a group server scan task in the Kaspersky Security Center Administration Console and assign it the "Critical Areas Scan task" status:*

1. Launch the group task creation wizard: in the Kaspersky Security Center Administration Console tree select the **Managed computers** node, select the group whose servers should create a task, open the context menu on the nested folder **Tasks** and select **New** → **Task**.
2. In the **Specify task name** window of the task creation wizard, enter the task name, for example Critical Areas scan on group servers.
3. In the **Task type** window under the heading **Kaspersky Security 10**, select the type of the task to be created: On-demand scan.
4. In the **Settings** window, select **New**.
5. In the **Scan scope** window change the scan scope, if required. By default, the scan scope includes the critical areas of the server.
6. In the **Options** window, select the **Consider task as Critical Areas scan** check box.
7. In the **Schedule** window configure the task schedule settings:
    a. check the **Run by schedule** box.
    b. Specify the frequency of starting the task, for instance once a week.
    c. Specify the time for the task launch in the **Start time** field.
    d. In the **Start date** field specify the current date as the date on which the schedule will be applied.
    e. Click **OK**.
8. In the **Finish** window of the task creation wizard press the **Ready** button.

This will create a group server scan task with a "Critical areas scan task" status.

Installing Kaspersky Security Console via Kaspersky Security Center

> Detailed information about creating an installation package and a remote installation task is provided in the *Kaspersky Security Center Implementation Guide*.

► *To install Kaspersky Security Console using a remote installation task:*

1. In the Kaspersky Security Center Administration Console expand the **Remote installation** node and in the nested **Installation Packages** node create a new installation package on the basis of the client\setup.exe file. While creating a new installation package:

   - In the **Select installation package type** window, select **Create an installation package for an application specified by the user** and select the client\setup.exe file from the distribution kit folder.

   - If required, modify the set of components to be installed using ADDLOCAL key in the **Executable file launch settings (optional)** field and change the destination folder.

     For instance, in order to install the Kaspersky Security Console alone in the folder C:\KasperskyConsole without installing the help file and documentation, proceed as follows:

     ```
     \server\setup.exe /s /p
     "ADDLOCAL=MmcSnapin INSTALLDIR=c:\KasperskyConsole
     EULA=1"
     ```

2. In the **Installation packages** node, create a task to remotely install Kaspersky Security Console on the selected computers (administration group). Configure task settings.

   To learn more about creating and configuring remote installation tasks, see *Administrator's Guide for Kaspersky Security Center*.

3. Run the remote installation task created.

The Kaspersky Security Console is installed on the computers specified in the task.

Uninstalling Kaspersky Security via Kaspersky Security Center

► *In order to uninstall Kaspersky Security, take the following steps in the Kaspersky Security Center Administration Console:*

1. In the Kaspersky Security Center Administration Console, create and start the application removal task.
2. In the task, select the deletion method (corresponds with the selection of the installation method; see previous item) and specify an account with the rights of which the Administration Server addresses the computers. You can uninstall Kaspersky Security only with default uninstallation settings (see section "Install and uninstall settings and their keys for the Windows Installer service" on page 29).

Installation and Uninstallation through active directory group policies

This section describes installing and uninstalling Kaspersky Security via Active Directory group polices. It also contains information about actions after installing Kaspersky Security through group policies.

In this section

Installing Kaspersky Security via Active Directory group policies

You can install Kaspersky Security on several servers via the active directory group policy. You can install Kaspersky Security Console in the same fashion.

Computers on which you wish to install Kaspersky Security (Kaspersky Security Console) must be in a single domain and a single organized unit.

The operating systems on the computers on which you wish to install Kaspersky Security with the help of the policy must be of the same version (32-bit or 64-bit).

You must have domain administrator rights.

To install Kaspersky Security, use the ks4ws_x86(x64).msi installation packages. To install Kaspersky Security Console, use the ks4wstools.msi installation packages.

> Detailed information about use of Active Directory group policies is provided in the documentation supplied by Microsoft.

► *To install Kaspersky Security (Kaspersky Security Console):*

1. Save the msi file of the installation package that corresponds to the word size (32- or 64-bit) of the installed version of the Microsoft Windows operating system, in the public folder on the domain controller.
2. On the domain controller create a new policy for a group in which servers are combined.
3. Using **Group Policy Object Editor** create a new installation package in the **Computer configuration** node. Specify the path to the msi file of the installation package of Kaspersky Security (Kaspersky Security Console) in the UNC format (Universal Naming Convention).
4. Select **Always install with elevated privileges** in Windows Installer service in both the **Computer configuration** node and in the **User configuration** node of the selected group.
5. Apply the changes with the `gpupdate / force` command.

Kaspersky Security will be installed on the computer group after they have been restarted, and before logging into Microsoft Windows.

Actions after installing Kaspersky Security

After installing Kaspersky Security on the protected servers, it is recommended that you immediately update the application databases and run a Critical Areas scan. You can perform these actions from Kaspersky Security Console (see section "Actions after installing Kaspersky Security" on page 61).

You can also configure administrator notifications about Kaspersky Security events (see the *Administrator's Guide for Kaspersky Security 10 for Windows Server*).

Kaspersky Security Uninstallation through active directory group policies

If you installed Kaspersky Security (Kaspersky Security Console) on the group computers using the Active Directory group policy, you may use this policy to uninstall the Anti-Virus (Kaspersky Security Console).

You can uninstall Anti-Virus only with default uninstall parameters.

> Detailed information about use of Active Directory group policies is provided in the documentation supplied by Microsoft.

► *To uninstall Kaspersky Security (Kaspersky Security Console):*

1. Select the organizational unit on the domain controller from whose computers you wish to delete Kaspersky Security or Kaspersky Security Console.

2. Select the policy created for the installation of Kaspersky Security and in the **Group policies editor**, in the **Software Installation** node (**Computer configuration** → **Program configuration** → **Software Installation**) open the context menu of the Kaspersky Security (Kaspersky Security Console) installation package and select the **All tasks** → **Remove** command.

3. Select deletion method **Delete program immediately** from all computers.

4. Apply the changes with the `gpupdate / force` command.

Kaspersky Security is removed from the computers after they are restarted and before logging in to Microsoft Windows.

Migrating from a previous version of the application

You can install Kaspersky Security 10 without uninstalling the previous version of the application if one of the following versions of Kaspersky Security is installed on your computer:

- Kaspersky Anti-Virus 6.0 for Windows Server MP4;
- Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

This section contains information on the capability to save, migrate, and apply settings of installed applications when installing Kaspersky Security 10 for Windows Server without removing Kaspersky Anti-Virus 6.0 for Windows Servers MP4 or Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

> The computer may have to be restarted when updating the program to Kaspersky Security 10 for Windows Server.

In this section

Migrating settings from Kaspersky Anti-Virus 6.0 for Windows Server MP4

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 and Kaspersky Security 10 for Windows Server are different applications and critically diverge in their sets of functional components and settings that you can configure.

When installing Kaspersky Security 10 over Kaspersky·Anti-Virus 6.0, you can partially migrate the following settings that were configured when working with Kaspersky·Anti-Virus 6.0:

- General application settings and settings of registered Windows services
- On-Demand Scan settings
- Trusted Zone settings
- Update settings

> After updating Kaspersky·Anti-Virus 6.0 to Kaspersky Security 10, you are advised to double-check the application settings that were migrated from Kaspersky·Anti-Virus to Kaspersky Security.

You can also apply policies and group tasks that were created when using Kaspersky·Anti-Virus 6.0 in Kaspersky Security.

> Kaspersky Security Center policies and group tasks are not automatically converted and are not supported without reinstalling the Kaspersky Security Administration Plug-in.

► *To use policies or group tasks that were created with Kaspersky·Anti-Virus 6.0,*

import the previously saved policy or task when creating a new policy or task during the first step of the Wizard in the Kaspersky Security 10 Plug-in.

Migrating settings from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 1

When migrating from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 1 to Kaspersky Security 10 for Windows Server, all local application settings are preserved without changes.

Kaspersky Security Center policies and group tasks are not automatically converted and are not supported without reinstalling the Kaspersky Security Administration Plug-in.

► *To use policies or group tasks that were created with Kaspersky·Anti-Virus 8.0,*

import the previously saved policy or task when creating a new policy or task during the first step of the Wizard in the Kaspersky Security 10 Plug-in.

Detailed information about the procedure for importing policies and group tasks is provided in the *Kaspersky Security 10 for Windows Server Administrator's Guide* and in the *Kaspersky Security Center Administrator's Guide*.

Checking Kaspersky Security functions use the EICAR test virus

This section describes the EICAR test virus and how to use the EICAR test virus to verify Kaspersky Security's Real-time protection and On-demand scan features.

In this section

About the EICAR test virus

The test virus is designed for verification of the operation of the anti-virus applications. It is developed by The European Institute for Computer Antivirus Research (EICAR).

> The test virus is not a virus and does not contain a program code that may damage to your computer, although most vendors' anti-virus applications identify a threat in it.

The file containing this test virus is called eicar.com. You can download it from the website of **EICAR** http://www.eicar.org/anti_virus_test_file.htm.

> Before saving the file in a folder on the computer’s hard drive, make sure that Real-Time File Protection on that drive is disabled.

File eicar.com contains a text line. When scanning the file Kaspersky Security detects a test threat in this text line, assigns the **Infected** status to this file and deletes it. Information about the threat detected in the file will appear in Kaspersky Security Console and in the task log.

You can use the eicar.com file in order to check how Kaspersky Security disinfects infected objects and how it detects probably infected objects. In order to do this, open the file using a text editor, add to the beginning of the text line in the file one of the prefixes listed in the table below, and save the file under a new name, for example eicar_cure.com.

> In order to make sure that Kaspersky Security processes the eicar.com file with a prefix, in the **Objects protection** security settings section, set the **All objects** value for the Kaspersky Security Real-Time File Protection tasks and Default On-demand Scan tasks. See the instructions in the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

Table 13. Prefixes in EICAR files

Prefix	File status after the scan and Kaspersky Security action
No prefix	Kaspersky Security assigns the **Infected** status to the object and deletes it.
SUSP–	Kaspersky Security assigns **Probably infected** status to the object (detected by the heuristic analyzer) and deletes it (probably infected objects are not disinfected).
WARN–	Kaspersky Security assigns **Probably infected** status to the object (the object's code partly matches the code of a known threat) and deletes it (probably infected objects are not disinfected).
CURE–	Kaspersky Security assigns the **Infected** status to the object and disinfects it. If disinfection is successful, the entire text in the file is replaced with world "CURE".

Checking the functions of Kaspersky Security Real-Time Protection and On-Demand Scan

After installing Kaspersky Security, you can confirm that Kaspersky Security finds objects containing malicious code. To check, you can use the test virus of **EICAR** (see section "**About the EICAR test virus**" on page 90).

► *In order to check the Real-Time Protection, take the following steps:*

1. Download file eircar.com from the **EICAR** site at http://www.eicar.org/anti_virus_test_file.htm. Save it into the public folder on the local drive of any of the computers on the network.

   > Before you save the file into the folder, make sure that the Real-Time File Protection is disabled in this folder.

2. If you wish to check the functioning of the user net notifications, make sure that the Microsoft Windows messaging service is enabled both on the protected server and on the computer on which you saved the file eicar.com.

3. Open Kaspersky Security Console

4. Copy the saved eicar.com file on the local drive of the protected server using the Remote Desktop Connection program:

   - To test notifications through the Terminal Services window, copy the file eicar.com to the server after connecting to the server using the Remote Desktop Connection utility;

   - To test notifications through Microsoft Windows NET SEND service, copy the file eicar.com from the computer where you saved it, via that computer's network places.

Real-Time File Protection works correctly if the following conditions are met:

- The file eicar.com has been deleted from the protected server.
- In the Kaspersky Security Console, the task log was given the status **Critical**. A line appeared in the log with information about a threat in the eicar.com file. (To view the task log, in the Kaspersky Security Console tree expand the **Real-Time Protection** node, select the Real-Time File Protection task and in the results panel of the node click the **Open log** link).
- A Microsoft Windows NET SEND message will have appeared on the computer from which you copied the file (or Terminal Service in the terminal session on the server), as follows: `Kaspersky Security blocked access to <path to file on the server>\eicar.com on computer <network name of computer> at <time that event occurred>. Reason: Threat detected. Virus: EICAR-Test-File. User name: <user name>. Computer name: <network name of the computer from which you copied the file>`.

> Make sure that Microsoft Windows NET SEND service is functioning on the computer from which you have copied the eicar.com file.

► *In order to check the On-Demand Scan function, take the following steps:*

1. Download file eircar.com from the **EICAR**site at http://www.eicar.org/anti_virus_test_file.htm. Save it into the public folder on the local drive of any of the computers on the network.

> Before you save the file into the folder, make sure that the Real-Time File Protection is disabled in this folder.

2. Open Kaspersky Security Console
3. Do the following:
   a. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
   b. Select the **Critical Areas Scan** subnode.
   c. On the **Scan scope settings** tab, open the context menu open the **Network** node and select **Add network file**.

d. Enter the network path to eicar.com file on the remote computer in the UNC format (Universal Naming Convention).

e. Check the box to include the added network path to the scan area.

f. Run the Critical Areas Scan task.

The on-demand scan works as it should if the following conditions are met:

- File eicar.com has been deleted from the computer disk.
- In the Kaspersky Security Console, the task log was given the status **Critical**; in the execution log of the task **Critical Areas Scan** a line appeared with information on a threat in the eicar.com file. (To view the task log, in the Kaspersky Security Console tree expand the **On-Demand Scan** subnode, select the **Critical Areas Scan** task and in the results panel click the **Open log** link).

Kaspersky Security deployment schemes

This section contains descriptions of schemes to deploy Kaspersky Security for the protection of DAS storages, clusters, terminal servers and network storages.

In this section

Protection of Directly Attached Storages (DAS)

Kaspersky Security protects data storage devices that are directly attached to the server (DAS storages) (see figure below).

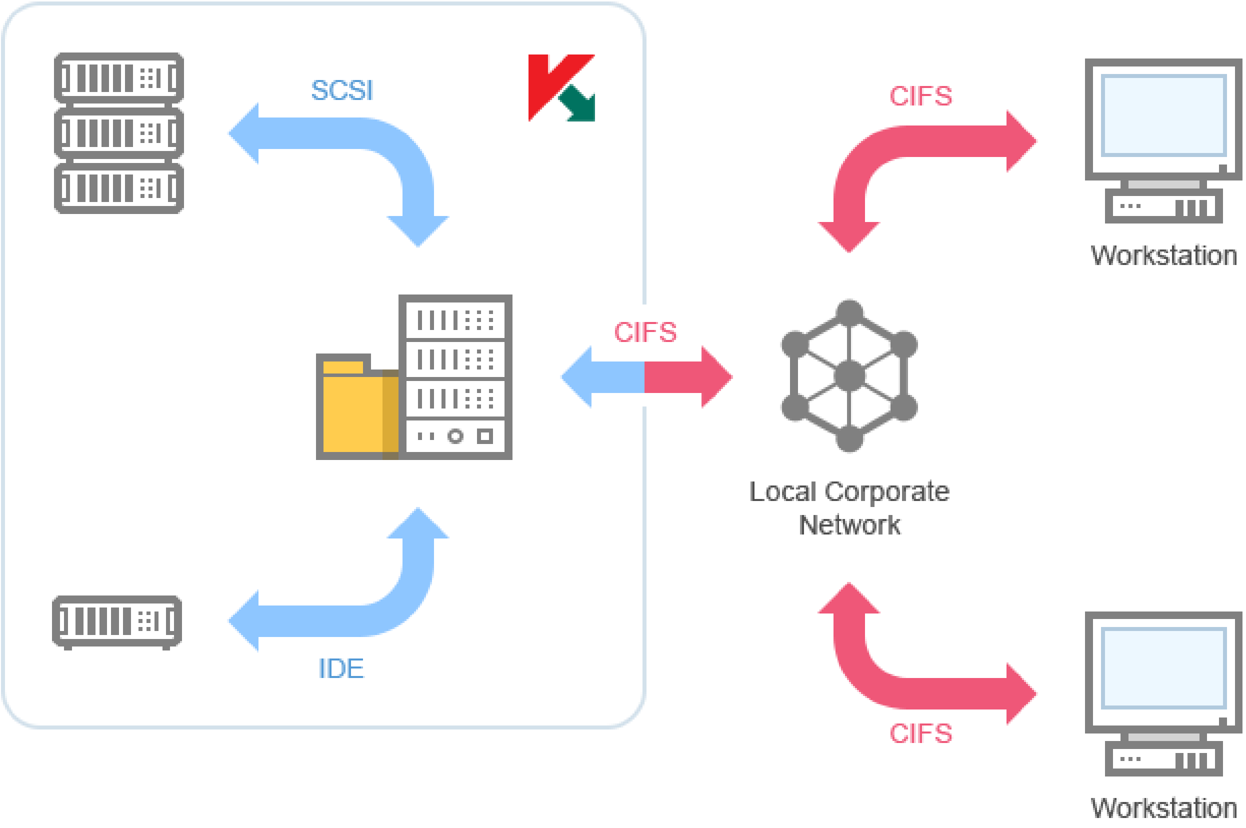

Figure 1. Block diagram of Directly Attached Storages protection

Kaspersky Security monitors file operations performed on files in DAS storages. Kaspersky Security recognizes DAS storages as local file resources of the server.

Protection of clusters

Kaspersky Security supports installation on server clusters running in **Active** / **Active** and **Active** / **Passive** modes (see figure below).

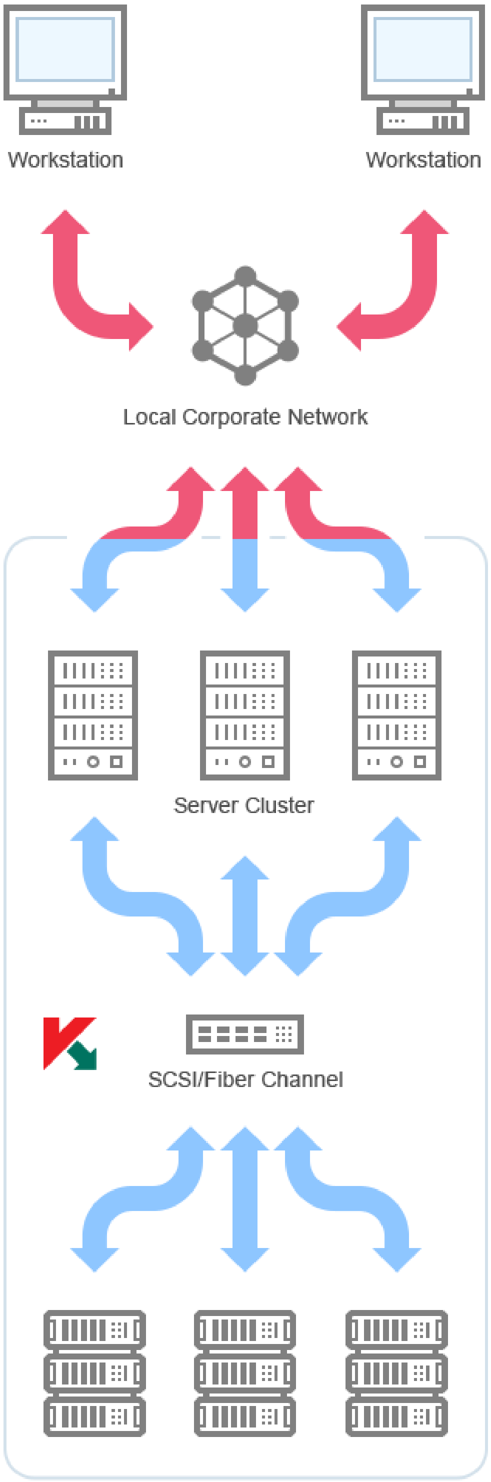

Figure 2. Block diagram of server cluster protection

Kaspersky Security ensures correct operation of the server during migration of cluster resources (**failover** / **failback**).

Complete cluster protection is achieved when Kaspersky Security is installed on each node. Kaspersky Security protects local drives of the server file system and shared drives of the cluster that are currently owned by the protected node. File resources owned by an unprotected cluster node are not protected.

Protection of terminal servers

Kaspersky Security protects terminal servers (see figure below).

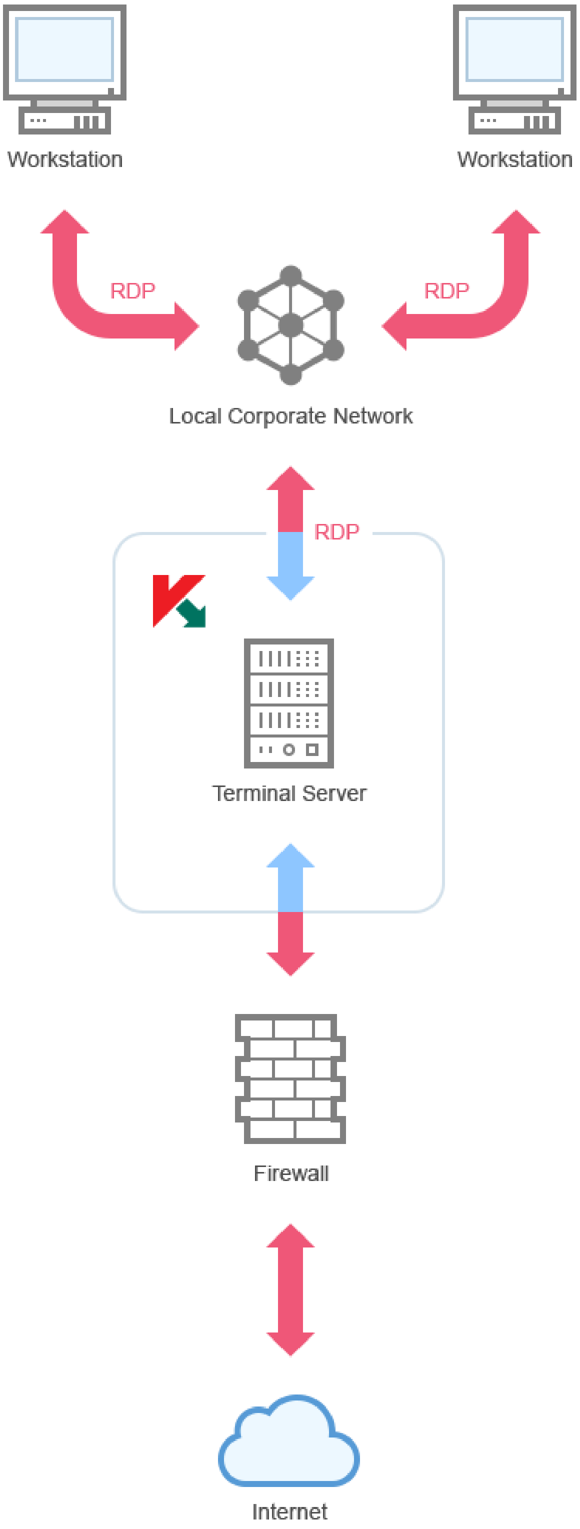

Figure 3. Block diagram of terminal server protection

Kaspersky Security includes the following features:

- Protection of terminal users working in the mode of desktop publication and app publication
- Notification of terminal users using terminal service tools
- Audit of operations performed on files and scripts of terminal users

Network Attached Storage Protection

Kaspersky Security installed on a server under a Microsoft Windows operating system protects network attached storages against viruses and other security threats that infiltrate the server through exchange of files.

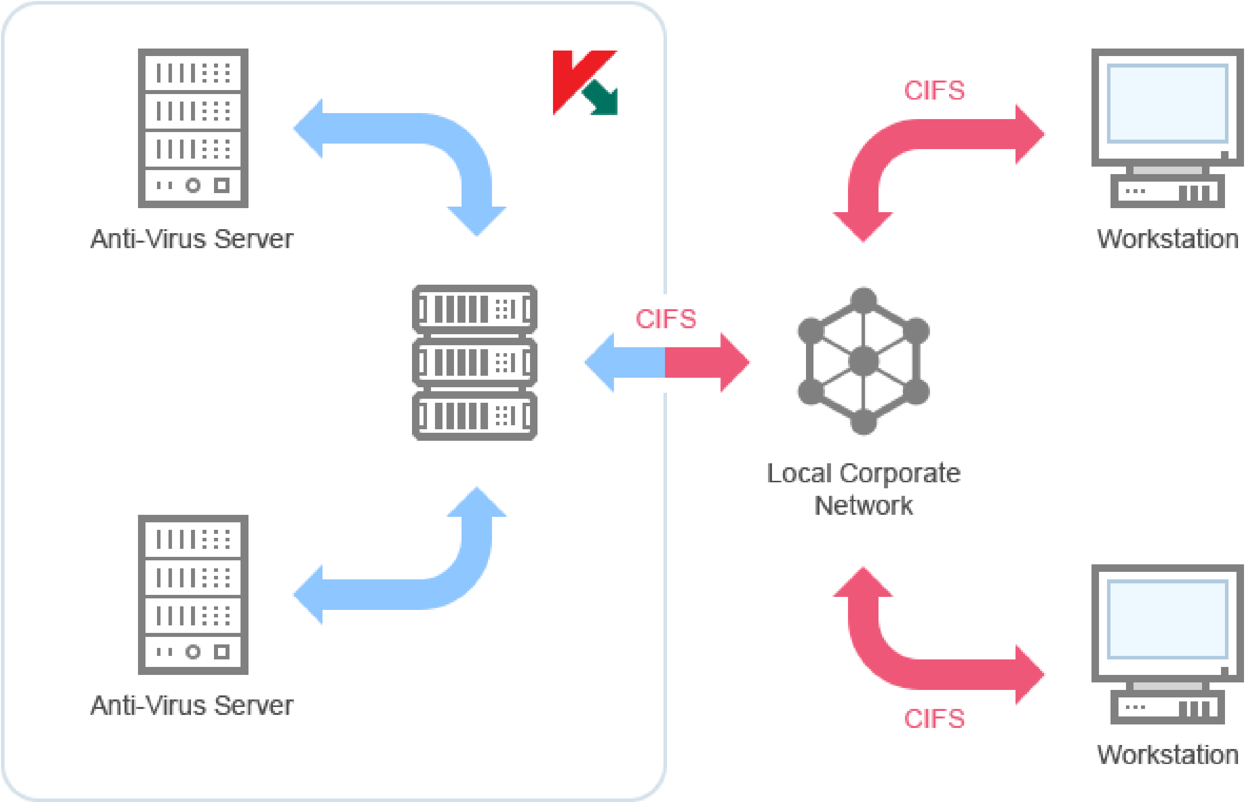

Figure 4. Network Attached Storage Protection scheme

Kaspersky Security scans files located in network share folders in the network storage system when an attempt is made to read or modify the files from a workstation. The network attached storage allows reading or modifying a file if Kaspersky Security has identified that file as safe. If Kaspersky Security has identified a file as infected or probably infected, the network attached storage blocks that file from being read or modified. Kaspersky Security allows you to configure the actions that the application will perform on infected and probably infected files. By default Kaspersky Security disinfects infected files, and if disinfection is not possible it deletes them (if the action is available in the network storage system); probably infected files are placed in quarantine. Before disinfecting or deleting a file, Kaspersky Security places a copy of the file in Backup.

You can find more detailed information in the *Implementation Guide for Kaspersky Security 10 for Windows Server for Network Storage Protection*.

Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

In this section

How to get technical support

If you cannot find a solution to your problem in the application documentation or in one of the sources of information about the application, we recommend that you contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is available only to users who have purchased a commercial license for the application. Technical support is not available to users who have a trial license.

> Before contacting Technical Support, please read through the Technical Support rules (http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By calling Technical Support (http://support.kaspersky.com/support/contacts)
- By sending a request to Technical Support through the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for companies that use Kaspersky Lab applications. Kaspersky CompanyAccount is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. Kaspersky CompanyAccount lets you monitor the progress of electronic request processing by Kaspersky Lab specialists and store a history of electronic requests.

You can register all of your organization's employees under a single user account on Kaspersky CompanyAccount. A single user account gives you centralized management of online requests from these employees to Kaspersky Lab, as well as control over the rights of these employees in your Kaspersky CompanyAccount.

Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

Technical support by phone

In most regions worldwide, you can contact Technical Support by phone. Information about how to contact Technical Support in your region is available on the Kaspersky Lab Technical Support website (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, please read through the Technical Support rules (http://support.kaspersky.com/support/rules).

Using trace files and AVZ scripts

After you report a problem to Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Security and to send it to Technical Support. Technical Support specialists may also ask you to generate a *trace file*. The trace file allows following the process of how application commands are performed, step by step, in order to determine the stage of application operation at which an error occurs.

After Technical Support Service specialists analyze the data that you have sent, they can create an AVZ script and send it to you. With AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.

Glossary

A

Network Agent

A component of Kaspersky Security Center that is responsible for interaction between Administration Server and Kaspersky Lab applications installed on a specific network node (workstation or server). This component is common for all Windows-based applications from the company's product range.

Active key

The key that the application currently uses in its operation.

Additional key

The additional key is a key that confirms the right to use the application but is not currently in use.

Administration group

A set of computers associated in accordance with their functions and the pool of Kaspersky Lab applications installed on them. Computers are grouped for the ease of management, which allows administering them as a single unit. A group may include other groups. Group policies and group tasks can be created for each of the applications installed within one group.

Administration server

A component of Kaspersky Security Center that performs centralized storage of information about Kaspersky Lab applications installed on the corporate network and ways of managing them.

Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky Lab as of the anti-virus database release date. Anti-virus database signatures help to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

Archive

A file that contains inside itself one or several other files, which, in their turn, may also be archives.

Application settings

Application settings that are common to all types of tasks and determine how the application operates in general. For example, performance, reports, and Backup settings.

B

Backup

A dedicated storage area intended for storing backup copies of files that have been created before their first disinfection or deletion.

D

Disinfection of objects

A method of processing infected objects that results in a complete or partial recovery of data. Not every infected object can be disinfected.

F

False alarm

A situation when a non-infected object is identified by a Kaspersky Lab application as infected because its code is similar to that of a virus.

H

Heuristic analysis

A technology intended for detection of threats that cannot be detected using current version of Kaspersky Lab applications databases. It allows finding files that may contain some unknown virus or a new modification of a known virus.

Files in which malicious code is detected during heuristic analysis are marked as *probably infected*.

Heuristic Analyzer

A technology of detecting threats whose signatures have not yet been added to Kaspersky Lab databases. The heuristic analyzer allows detecting objects behaving in a way that can pose a security threat to the operating system. Objects detected by the heuristic analyzer are considered probably infected. For example, an object may be considered probably infected if it contains sequences of commands that are typical of malicious objects (open file, write to file).

I

Infected file

A file that contains malicious code (i.e., when scanning the file, code of a known application that poses a threat has been detected). Kaspersky Lab specialists recommend that you abstain from handling such files since this may lead to an infection of your computer.

K

Key file

An xxxxxxxx.key file that makes it possible to activate a Kaspersky Lab application on the terms of a license by adding a key.

M

File mask

Representation of the name and extension of a file by means of wildcards.

To create a file mask, you can use any symbols that are allowed to use in file names, including special ones:

- ***** – the symbol that substitutes zero or more characters
- **?** – the symbol that substitutes any single character

Please note that the name and the extension of a file are always separated with a dot.

O

OLE object

A file that has been merged or integrated into another one. Kaspersky Lab applications allow scanning OLE objects for viruses. For example, if you embed a Microsoft Office Excel® spreadsheet into a Microsoft Office Word document, the former will be scanned as OLE object.

P

Potentially infectable file

A file with a specific structure or format that may be used by criminals to convert this file into a container for storing and spreading malicious code. As a rule, they include executable files, for example, those with com, exe, dll, and other similar extensions. The risk of malicious code penetration into such files is rather high.

Probably infected file

A file that contains either modified code of a known virus, or code that is similar to one but still unknown to Kaspersky Lab. Probably infected files can be detected by the means of the heuristic analyzer.

Q

Quarantine

The folder to which the Kaspersky Lab application moves probably infected objects that have been detected. Objects are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

S

Signature analysis

Threat detection technology, which uses Kaspersky Security databases that contain the descriptions of known threats and the methods of neutralizing them. Protection with signature analysis ensures the minimum admissible security level. According to recommendations of Kaspersky Lab specialists, this analysis method is always enabled.

Startup objects

A set of applications that are required for start and proper operation of the operating system and software installed on the computer. Every time the operating system boots, it runs those objects. There are viruses aimed at infecting such objects, which may result, for example, in blocked booting of the operating system.

T

Task

Functions performed by the Kaspersky Lab application as tasks, for example: Real-Time File Protection, Full scan, Application databases update.

Task settings

Settings of the application that are specific for each task type.

U

Update

A procedure that consists in replacing / adding new files (databases or application modules) retrieved from Kaspersky Lab update servers.

V

Vulnerability

A flaw in the operating system or in an application that may be exploited by malicious programs in order to intrude into the operating system or application and corrupt its integrity. A large number of vulnerabilities in the operating system makes its operation unreliable, because viruses that have intruded into the operating system may provoke failures in the system's operation or errors in the operation of installed applications.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems for protection of computers against various threats, including viruses and other malware, spam, network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). In Russia, according to IDC, Kaspersky Lab is the first choice among vendors of computer protection systems for home users (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company is now employing more than 3,000 skilled professionals.

PRODUCTS. Kaspersky Lab products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes information security applications for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

The company offers solutions and technologies for protection and control of workstations and mobile devices, virtual machines, file servers and web servers, mail gateways, and firewalls. The company's portfolio also includes dedicated products for protection against DDoS attacks, protection of environments managed with industrial control systems, and fraud prevention. Used in conjunction with centralized management tools, these solutions ensure effective automated protection against computer threats for companies and organizations of any scale. Kaspersky Lab products are certified by major testing laboratories, compatible with the applications of most software vendors, and optimized for work on most hardware platforms.

Kaspersky Lab virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include the signatures of these threats in the databases used by Kaspersky Lab applications.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that the program kernel of Kaspersky Anti-Virus is integrated in products of many software vendors, including Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2014, tests and researches conducted by the renowned Austrian anti-virus lab AV-Comparatives brought Kaspersky Lab one of the two leading positions in the number of Advanced+ certificates awarded, which gave the company the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website:	http://www.kaspersky.com
Virus Encyclopedia	http://www.securelist.com/
Virus Lab:	http://newvirus.kaspersky.com (for scanning suspicious files and websites)
Kaspersky Lab web forum:	http://www.kaspersky.com

Information about third-party code

Information about third-party code is contained in a file named legal_notices.txt and stored in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Citrix, XenApp, and XenDesktop are registered trademarks of Citrix Systems, Inc. and/or subsidiaries in the United States and/or elsewhere.

Celerra, EMC, Isilon, OneFS, and VNX are either registered trademarks or trademarks of EMC Corporation in the United States and/or elsewhere.

Radmin are registered trademarks of Famatech.

Domino, IBM, Lotus Notes, System Storage are trademarks of International Business Machines Corporation registered all over the world.

Active Directory, Hyper-V, Excel, Microsoft, Windows, Windows Server, Windows Vista are trademarks of Microsoft Corporation registered in the United States and elsewhere.

Data ONTAP and NetApp are either registered trademarks or trademarks of NetApp, Inc. in the United States and/or elsewhere.

Index